

Beta Privacy Addendum (B2B)

BETA PRIVACY ADDENDUM (DIAGNOSTICS & TELEMETRY) This Beta Privacy Addendum ("Addendum") forms part of the Beta Program agreement ("Agreement") between ARRI GmbH ("Provider") and the entity or individual participating in the Beta Program ("Customer"). Capitalized terms not defined here have the meaning in the Agreement.

1. Purpose and scope

1.1 Provider provides Customer with access to a pre-release ("Beta") version of **ARRI Reference Tool Viewer** (the "Beta Software").

1.2 This Addendum describes the processing of **Diagnostics & Telemetry Data** generated when using the Beta Software and transmitted to Provider and/or its service providers for the purposes of quality assurance, stability, security, and support.

2. Definitions

2.1 **Diagnostics & Telemetry Data** means technical and usage data generated by the Beta Software, limited to the categories listed in Section

2.2 **Personal Data** has the meaning set forth in the GDPR (Regulation (EU) 2016/679). 2.3 **Sentry** means the error monitoring service provided by Sentry (or an affiliated entity) used by Provider as described in Section 5.

3. Data categories (data minimization)

Provider will collect and process only the minimum diagnostics data necessary to operate and improve the Beta Software, including:

- **Runtime errors and crash reports** (exception type, stack trace, error message, build/version, platform/OS, timestamp).
- **Operational metrics** (e.g., session duration in coarse granularity, feature flags used, high-level usage counters).
- **Environment metadata** (application version, operating system version, device class/type, locale, time zone, performance class where applicable).

- **Connectivity/transport metadata** strictly necessary for delivery (e.g., success/failure codes; **no IP address storage** as per Section 4).
- **User-provided data** submitted via the feedback form, in particular:
 - Email address
 - Name
 - Message text

Provider will **not intentionally collect**:

- names, phone numbers, addresses, or other direct identifiers;
- content data processed by Customer in production systems;
- secrets/tokens/passwords;
- full request/response payloads unless Customer explicitly enables a debug mode in writing.

4. IP addresses and identifiers

4.1 Provider configures telemetry so that **IP addresses are not stored** in Provider's telemetry systems where technically feasible.

4.2 Provider will avoid persistent device identifiers. If a diagnostic identifier is required, Provider will use a **pseudonymous, tenant-scoped** identifier and may rotate or reset it.

5. Service providers and locations

5.1 Provider uses **Sentry** as a diagnostics processor to collect and analyze crash and error events.

5.2 Sentry acts as **processor** to Provider for Diagnostics & Telemetry Data. Provider will maintain an appropriate **data processing agreement (DPA)** with Sentry and ensure Sentry provides appropriate technical and organizational measures.

5.3 Where processing involves transfers outside the EEA/UK/Switzerland, Provider will implement an appropriate transfer mechanism (e.g., **SCCs** and/or other valid transfersafeguards, as applicable).

6. Roles and responsibilities

6.1 Controller / Processor. Provider is controller for Diagnostics & Telemetry Data processedfor Provider's purposes (quality, stability, security, support). Customer is controller for anyCustomer content data and any Personal Data embedded in Customer logs/content.

6.2 Customer shall not intentionally submit Personal Data or Customer confidential content inbug reports, logs, or attachments unless strictly necessary and approved by Customer.

7. Security measures

Provider will apply reasonable security measures appropriate to risk, including:

- encryption in transit (TLS) and at rest (where supported),
- access controls and least-privilege access to telemetry,
- logging/audit trails for administrative access (where supported),
- environment separation for Beta projects (where feasible),
- regular patching and vulnerability management.

8. Retention and deletion

8.1 Provider will retain Diagnostics & Telemetry Data for 90 days by default, unless longerretention is required for active investigation, legal requirements, or security incident handling.

8.2 Upon Customer's written request and where technically feasible, Provider will deleteDiagnostics & Telemetry Data associated with Customer's Beta usage, subject to legal andoperational constraints.

9. Optional settings and user notice

9.1 Provider will provide a configuration setting (e.g., "Include diagnostic data") allowing Customer to enable/disable non-essential telemetry.

9.2 Provider will document the telemetry categories and configuration in the Beta documentation.

10. Contact and requests

For privacy/security inquiries related to Beta diagnostics, Customer may contact: privacy@arri.de.